374

Lecture 2: Reductions

8/26/21

$X \leq Y$ ≡ there is a reduction from X to Y.

X, Y: Problems

I_X: Input of problem X
Instance of X

Reduction from X to Y

I_X → [reduction] → I_Y

I_X is a yes instance of X ⟺ I_Y is a yes instance of Y

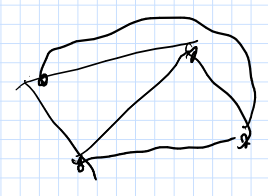
$n = |I_X|$ ↑ Running time of the reduction is polynomial

$RT \leq O(n^c)$ c is a constant

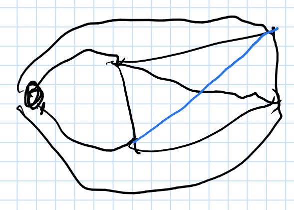
$X \leq_P Y$ Poly time reduction from X to Y.

Clique problem

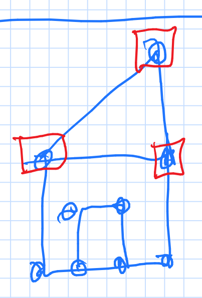
I: Undirected graph G. And a number k.
Q: Does G contains a clique of size k?



K_4



K_5

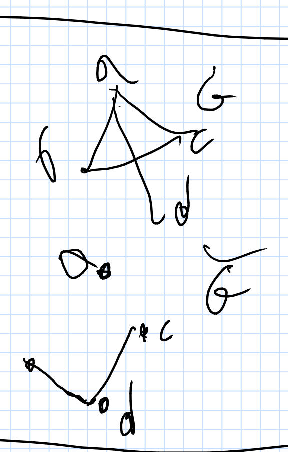


Decision problem: yes/no
Seach problems: return a clique
Optimization problem: return the best solution

Independent set

A set $S \subseteq V(G)$ is independent ⟺ no pair of vertices of S are connected by an edge.

$G = (V, E)$
$\bar{G} = (V, \bar{E} = \{uv \mid u, v \in V, uv \notin E\})$



Lemma

G has a clique of size k
⟺
$\bar{G}$ has an independent set of size k.

Clique $\leq_P$ Independent set

$I_C: \langle G, k \rangle$ → [reduction IS] → $\langle \bar{G}, k \rangle$
computes $\langle \bar{G}, k \rangle$

Conclusion
Clique $\leq_P$ IndependentSet
IndependentSet $\leq_P$ Clique

$IS \equiv_P$ Clique

$X \leq_P Y$

[I_X] — [reduction to Y] —I_Y→ [solver for Y] →

X is hard (can not be solved in poly time)

$X \leq_P Y$
⇓
Y must also be "hard".

Claim

X, Y decision problems
$X \leq_P Y$
X can not be solved in polynomial time.
⟹
Y can not be solved in polynomial time

Proof

Assume for contradiction this is false.
Y can be solved in poly time
A_Y be the algorith.

I_X ⟹ [poly time reduction] —I_Y→ [A_Y] $n = |I_X|$
$X \leq_P Y$ $f(m) = O(m^\alpha)$

$|I_Y| = O(n^c)$ α, c is some constant

Running A_Y on I_Y is going to take

$$O(f(|I_Y|)) = O((|I_Y|)^\alpha) \leq O((n^c)^\alpha) = O(n^{c\alpha})$$

polynomial!

⟹ Contradiction
got poly time solver for X. ∎

A **verifier/certifier** is an alg for a decision problem s.t. given a "yes" instance I and a "proof" ("the solution") C the verifier can in poly time verify that I is indeed a yes instance.

certifier(I, C) → yes / no

output yes ⟺ I is a yes instance and C is a valid certificate

$|C| = O(n^c)$ c is a constant
$n = |I_X|$.

NP = Non-deterministic polynomial time

P = All decisions problems that can be solved in polynomial time.

P = NP   **P ≠ NP**